

Data Security, Data Breaches, and Liability



UNC
SCHOOL OF GOVERNMENT

www.sog.unc.edu

Shannon H. Tufts,
tufts@sog.unc.edu
Maurice Ferrell,
mferrell@sog.unc.edu

Cyber Intrusions are a Fact of Life

]HackingTeam[

UCLA Health System

ASHLEY
MADISON®
Life is short. Have an affair.®



U B E R



PlayStation Network



JPMORGAN CHASE & CO.



Forbes



Anthem®

ebay

Toys R Us



Targeted Attacks are Hard to Detect

How are compromises detected?

69%

of victims were notified
by an external entity

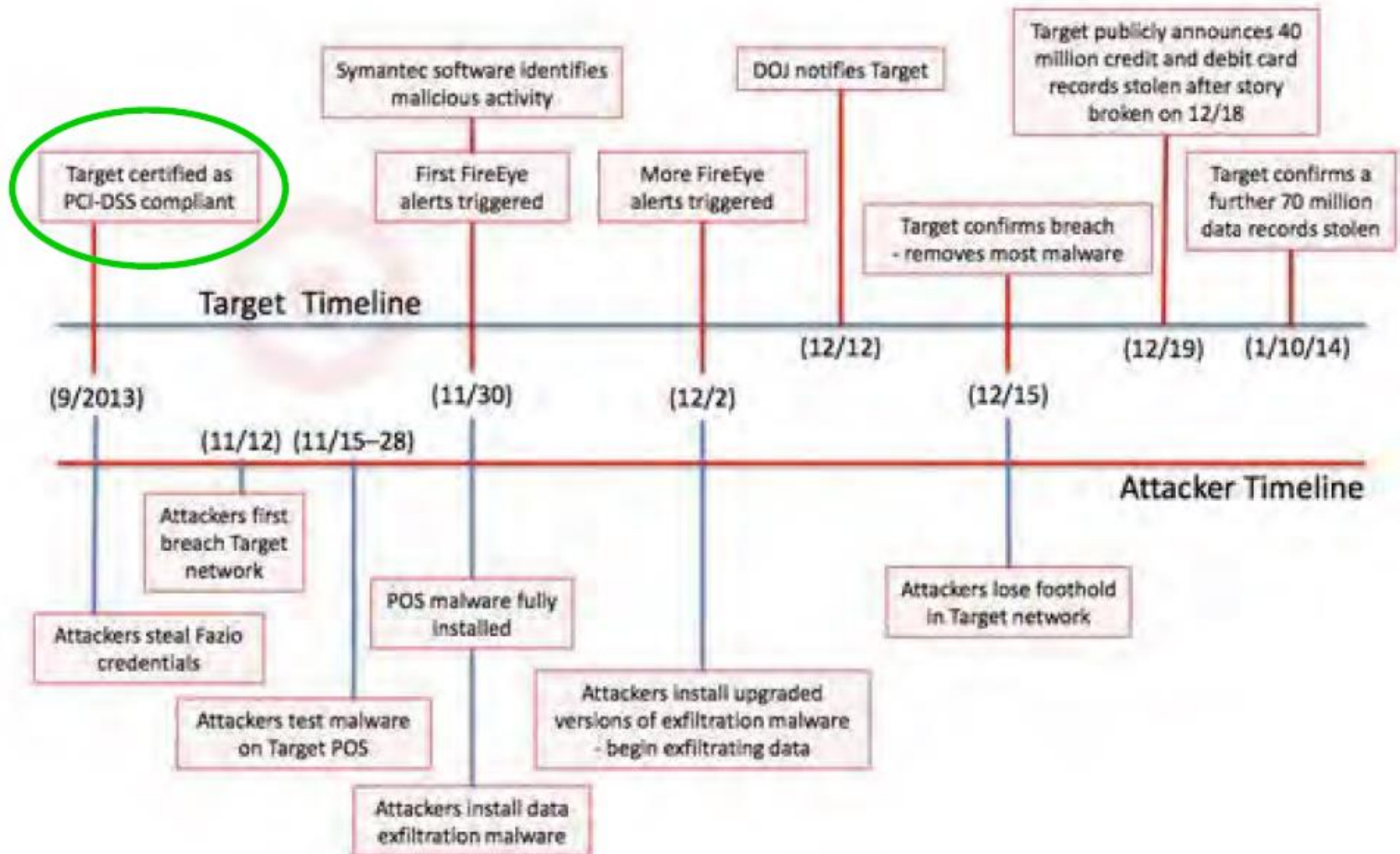
How long before the
compromises are
detected?

205

median number of days
before detection

SOURCE: Mandiant® "M-Trends® 2015: A View from the Front Lines" Report

Timeline of the Target Data Breach



Source: <https://www.idradar.com/news-stories/identity-protection/Target-Dropped-The-Ball-On-Breach-Detection-Report-Says>

Key Lessons From Target

- Reconnaissance performed via “case studies”
- Back door access from third-party vendor
- People = weakest link
- Contract requirements related to security necessary
- Compliance does not equal security
- Security is a C-level issue, not just an IT issue

Bloomberg study key findings

Companies including utilities, banks, and phone carriers would have to spend almost nine times more to stop 84% of cyber attacks, up from 69%

Government is most vulnerable—stopping only 67%

Bloomberg
GOVERNMENT



Target = \$46.6B

Current = \$5.3B



Liability, Costs, Insurance

\$3.79 million

average cost per breach in 2015

April 2014

Fed policy covers breaches that occur
after signed policy date

\$2 million

Washington's cyber insurance annual
and incident max

Dec 2013

Date of OPM breach

60+%

breaches linked to 3rd party component of
IT system admin

Contracts Matter!



8.1. Limited Warranty; Limitation on Liability. Intermedia provides the Services and any related products on an “as is” basis. ... Intermedia and the Intermedia Parties will not be liable for any direct, indirect, incidental, special, punitive or consequential damages (including but not limited to damages for lost profits, business interruption, loss of programs or information, and the like) that result from the use or inability to use the Services or from mistakes, the Services not meeting Your requirements or expectations, omissions, hardware failures, translations and system wordings, functionality of filters, migration issues, interruptions, deletion of files or directories, unavailability of backups, errors, defects, delays in operation, or transmission, regardless of whether Intermedia or any Intermedia Party has been advised of such damages or their possibility. ...Your sole remedy for any claims regarding the Services under this Agreement or otherwise is limited to any applicable credits set forth in the Service Level Agreement.

Culture Matters Too!



#TRUTH

*...there are only two types of companies:
those that have been hacked and those that
will be...*

*...and even they are converging into
one category: companies that have
been hacked and will be hacked
again...*

*Robert S. Mueller, III
Former Director of FBI
March 1, 2012*